IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 30, 2021, accepted May 20, 2021, date of publication October 4, 2021, date of current version October 15, 2021.
Digital Object Identifier 10.1109/ACCESS.2021.3117561

Some Classes of New Quantum MDS and Synchronizable Codes Constructed From Repeated-Root Cyclic Codes of Length $6p^s$

HAI Q. DINH[1,2], HA T. LE[3], BAC T. NGUYEN[4,5], AND PARAVEE MANEEJUK[6]
[1]Division of Computational Mathematics and Engineering, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[2]Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[3]Department of Basic Sciences, Thai Nguyen University of Economics and Business Administration, Thai Nguyen 250000, Vietnam
[4]Institute of Fundamental and Applied Sciences, Duy Tan University, Ho Chi Minh City 700000, Vietnam
[5]Faculty of Natural Sciences, Duy Tan University, Da Nang 550000, Vietnam
[6]Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, Chiang Mai 50200, Thailand

Corresponding author: Bac T. Nguyen (nguyentrongbac@duytan.edu.vn)

This work was supported in part by the Research Administration Centre, Chiang Mai University. The work of Hai Q. Dinh and Paravee Maneejuk was supported in part by the Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University.

ABSTRACT In this paper, we use the CSS and Steane's constructions to establish quantum error-correcting codes (briefly, QEC codes) from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$. We obtain several new classes of QEC codes in the sense that their parameters are different from all the previous constructions. Among them, we identify all quantum MDS (briefly, qMDS) codes, i.e., optimal quantum codes with respect to the quantum Singleton bound. In addition, we construct quantum synchronizable codes (briefly, QSCs) from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$. Furthermore, we give many new QSCs to enrich the variety of available QSCs. A lot of them are QSCs codes with shorter lengths and much larger minimum distances than known non-primitive narrow-sense BCH codes.

INDEX TERMS Cyclic codes, negacyclic codes, MDS codes, CSS construction, Steane construction, Hermitian construction, quantum MDS codes, quantum synchronizable codes.

I. INTRODUCTION

An $[n, k]$ linear code C over $\mathbb{F}_{p^m}$ is a k-dimensional subspace of $\mathbb{F}_{p^m}^n$, where p is a prime number and $\mathbb{F}_{p^m}$ is a finite field. Let C be a linear code of length n over $\mathbb{F}_{p^m}$. Then C is called a λ-*constacyclic code* if it is an ideal of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n-\lambda\rangle}$. If $\lambda = 1, -1$, those λ-constacyclic codes are called *cyclic codes, negacyclic codes*, respectively.

In 1959, cyclic codes over finite fields were first studied by Prange [66]. In 1967, [3] studied the case $(n, p) = 1$ and such codes when $(n, p) = 1$ are so-called repeated-root codes. After that, [62] and [68] also considered repeated-root codes. They are optimal in a few cases, that motivates researchers to further study this class of repeated-root constacyclic codes over finite fields, and even more generally, over finite commutative chain rings (see, e.g., [8]–[11], [12]–[15], [16]).

Recently, Dinh ([24]–[26]), studied the structure of all constacyclic codes of lengths $2p^s$, $3p^s$ and $6p^s$ over $\mathbb{F}_{p^m}$. He also discussed about dual constacyclic codes of these lengths. In 2014, [18] determined the structure of codes of length lp^s over $\mathbb{F}_{p^m}$.

Let $C = [n, k, d_H]_q$ be a code. Then [60] showed that n, k, d_H must satisfy $k \le n - d_H + 1$ (the Singleton bound). If $k = n - d_H + 1$, then C is called a *maximum-distance-separable (briefly, MDS) code*. The problem of constructing MDS codes is a hot topic because an MDS code has the greatest detecting and error-correcting capabilities.

In 1985, Deutsch [22] gave an idea that computers use quantum bits (briefly, *qubit*) to solve certain problems, including prime factorization, exponentially faster than classical computers. Similar to classical bits, a qubit can be defnied as $|\varphi\rangle = z_1|0\rangle + z_2|1\rangle$, where $z_1, z_2 \in \mathbb{C}$ are complex numbers such that $|z_1|^2 + |z_2|^2 = 1$.

By empirical evidence, we cannot use classical error-correcting codes in quantum computation. However, A class of codes is proposed to protect quantum information that is the class of QEC codes. In 1995, in the paper [72], Shor first introduced QEC codes. And then Hamming codes, BCH

The associate editor coordinating the review of this manuscript and approving it for publication was A. Taufiq Asyhari.

codes and Reed-Solomon codes are used to construct many QEC codes. By applying the idea in [2], [6], [54], [72], [76], QEC codes have been studied extensively (for example, [2], [7], [20], [37], [53]). Recently, using [72] and [6], some QEC codes are constructed from the CSS and Hermitian constructions.

Since qMDS codes have great applications in quantum computation and quantum communication, constructing qMDS code has become an important topic. Therefore, some authors used graph theory to construct qMDS codes [39], [44], [69], [70]. In addition, applying the classical codes, some qMDS codes were constructed [19], [43], [49]. In 2009, [43] gave a class of qMDS codes from cyclic codes. After that, [49] gave two new classes of qMDS codes from negacyclic codes in 2013. Recent years, many researchers worked on construction of qMDS code with minimum distance larger than $\frac{q}{2}+1$ (for examples, [19], [30], [31], [71], [82], [83]).

An $[[n, k]]$ QEC code encodes k logical qubits into n physical qubits. An $(a_b, a_e) - [[n, k]]$ QSC is an $[[n, k]]$ quantum error-correcting code that corrects not only bit errors and phase errors but also misalignment to the left by a_b qubits and to the right by a_e qubits for some non-negative integers a_b and a_e.

Block synchronization is an important problem in classical digital communications which was studied in [4], [33], [55], [63], [65], [74]. However, in quantum information, the methods in [4], [33], [55], [63], [65], [74] don't apply. Therefore, Fujiwara [32] first proposed QSCs to correct both quantum noise and block synchronization errors. After that, [58] proposed a class of QSCs from repeated-root codes using the CSS construction.

In [27], we studied qMDS codes from negacyclic and cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$. We also gave some QSCs constructed from cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$. However, in [27], we did not find some QEC codes using the CSS and Steane's constructions. In this paper, we construct some new QEC codes from cyclic codes of length $6p^s$ using the CSS and Steane's constructions and some new QSCs from cyclic codes of length $6p^s$. By applying the CSS construction, we also provide all qMDS codes built from cyclic codes of length $6p^s$. Note that the structure of codes of length $6p^s$ is much more complicated than cyclic and negacyclic codes of length $2p^s$. Repeated-root cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ form a very interesting class of constacyclic codes. Their algebraic structures in term of generator polynomials were provided in 2014 in [26]. Recently, these structures were used in [28] to completely determine the Hamming distances of all such cyclic codes.

Motivated by these, in this research, we construct QEC codes from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using CSS and Steane's constructions. Especially, we compare our QEC codes with all previous QEC codes to show that some our QEC codes are new in the sense that their parameters are different from all the previous results. We also provide all qMDS codes from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using the CSS construction. Furthermore, we also construct QSCs from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$.

This paper is organized as follows. Section 2 gives some basic results. Section 3 constructs QEC codes from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using the CSS and Steane's constructions. Section 4 studies qMDS codes from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using the CSS construction. Section 5 constructs QSCs from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$. Section 6 gives some examples to illustrate our results in Sections 3, 4 and 5, where we present numerous qMDS and QSCs codes. Section 7 concludes our paper with some possible open direction for future studies.

II. PRELIMINARIES

The following lemma is given in [60].

Lemma 1 (cf. [60]): Let C be a linear code of length n over $\mathbb{F}_{p^m}$. Then C is λ-constacyclic over $\mathbb{F}_{p^m}$ if and only if C is an ideal of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n-\lambda\rangle}$.

Given n-tuples

$$u = (u_0, u_1, \ldots, u_{n-1}),\ v = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_{p^m}^n,$$

the inner product (dot product) of two vectors u, v is defined:

$$u \cdot v = u_0v_0 + u_1v_1 + \cdots + u_{n-1}v_{n-1},$$

evaluated in $\mathbb{F}_{p^m}$. If $u \cdot v = 0$, then two vectors u, v are called *orthogonal*. Dual code of a linear code C over $\mathbb{F}_{p^m}$, denoted by $C^\perp$, is defined as follows:

$$C^\perp = \{u \in \mathbb{F}_{p^m}^n \mid u \cdot v = 0, \quad \forall v \in C\}.$$

The result on the dual of a Λ-constacyclic code is provided in [23] as follows.

Proposition 2 (cf. [23]): The dual of a Λ-constacyclic code is a Λ^{-1}-constacyclic code.

In [26], Dinh studied cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$. We recall the structure of cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ when $p^m \equiv 2 \pmod 3$.

Theorem 3 ([26, Theorem 3.2]): Assume that $p^m \equiv 2 \pmod 3$. All cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ which are of the form $\langle h_0(x)^{u_0}h_1(x)^{u_1}h_2(x)^{u_2}h_3(x)^{u_3}$, where $0 \leq u_t \leq p^s$ $(t = 0, 1, 2, 3)$. Each code $C = \langle h_0(x)^{u_0}h_1(x)^{u_1}h_2(x)^{u_2}h_3(x)^{u_3}$ contains $p^{m(6p^s-u_0-u_1-2u_2-2u_3)}$ codewords, its dual $C^\perp$ is the cyclic code $C^\perp = \langle h_0(x)^{p^s-u_0}h_1(x)^{p^s-u_1}h_2(x)^{p^s-u_2}h_3(x)^{p^s-u_3}$, where $h_0(x) = x-1$, $h_1(x) = x+1$, $h_2(x) = x^2-x+1$, $h_3(x) = x^2+x+1$.

We recall the definition of QEC codes appeared in [67].

Definition 4 [67]: Let $q = p^m$ and $H_q(C)$ be a q-dimensional Hilbert vector space. Denote $H_q^n(C) = H_q(C)\otimes\cdots\otimes H_q(C)$ (n times). A quantum code of length n and dimension k over $\mathbb{F}_q$ is defined to be a q^k dimensional subspace of $H_q^n(C)$ and simply denoted by $[[n, k, d_H]]_q$, where d_H is the Hamming distance of the quantum code.

We give a small lemma.

Lemma 5: Let $0 < t \in \mathbb{N}$. Then there are $\frac{(t+2)(t+1)}{2}$ pairs of non-negative integers x, y such that $x + y \leq t$.

Proof: If $x = 0$, then we have $t+1$ options for y. If $x = 1$, then we have t options for y. In general, for any $x = j$, where

$0 \leq j \leq t$, there are $t-j+1$ options for y. That means y can be any integer from 0 to $t-j$. It implies that there are $1+2+3+\cdots+t+(t+1) = \frac{(t+2)(t+1)}{2}$ pairs of non-negative integers x, y such that $x+y \leq t$. □

III. QUANTUM CODES FROM CYCLIC CODES OF LENGTH $6p^s$ OVER $\mathbb{F}_{p^m}$

In 1995, QEC codes were first introduced by Shor [72]. After that, in 1996, by using the structure of classical codes over GF(4), [6] found some QEC codes. In 1998, [7] gave a new method to construct QEC codes from classical codes. Recently, [2], [7], [20], [37], [53] constructed some QEC codes over finite fields and some classes of finite rings. However, QEC codes constructed from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using the CSS and Steane's constructions have not been studied in the past.

We recall a construction of QEC codes, the so-called CSS construction.

Theorem 6 (CSS Construction [6]): Let $C_1 = [n, k_1, d_1]_q$ and $C_2 = [n, k_2, d_2]_q$ be two linear codes satisfying $C_2 \subseteq C_1$. Then there exists a QEC code with the parameters $[[n, k_1 - k_2, \min\{d_1, d_2^{\perp}\}]]_q$, where $d_2^{\perp}$ is the Hamming distance of the dual code $C_2^{\perp}$. Moreover, if $C_2 = C_1^{\perp}$, then there exists a QEC code with the parameters $[[n, 2k_1 - n, d_1]]_q$.

Throughout this paper, $p^m \equiv 2 \pmod 3$. Recall that C is *dual-containing* if $C^{\perp} \subseteq C$. We give the condition of a cyclic code of length $6p^s$ over $\mathbb{F}_{p^m}$ to be dual-containing to construct QEC codes.

Proposition 7: Let C be a cyclic code of length $6p^s$ over $\mathbb{F}_{p^m}$ which is of the form $\langle h_0(x)^{u_0} h_1(x)^{u_1} h_2(x)^{u_2} h_3(x)^{u_3} \rangle$, where $0 \leq u_t \leq p^s$ $(t = 0, 1, 2, 3)$, where $h_0(x) = x - 1, h_1(x) = x+1, h_2(x) = x^2 - x + 1, h_3(x) = x^2 + x + 1$. Then $C^{\perp} \subseteq C$ if and only if $0 \leq u_t < \frac{p^s}{2}$. In addition, the number of dual-containing codes is $(\frac{p^s+1}{2})^4$.

Proof: By Theorem 3, it is easy to see that $C^{\perp} = \langle h_0(x)^{p^s-u_0} h_1(x)^{p^s-u_1} h_2(x)^{p^s-u_2} h_3(x)^{p^s-u_3} \rangle$. Hence, $C^{\perp} \subseteq C$ if $p^s - u_t \leq u_t$ $(t = 0, 1, 2, 3)$. It means that $0 \leq u_t < \frac{p^s}{2}$ $(t = 0, 1, 2, 3)$. We see that $\frac{p^s+1}{2}$ values to choose u_t $(t = 0, 1, 2, 3)$. Hence, the number of dual-containing codes is $(\frac{p^s+1}{2})^4$. □

Recently, [28] studied the Hamming distance of cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$. So, we can determine all Hamming distances of cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ when $p^m \equiv 2 \pmod 3$. Combining Proposition 7 and Theorem 6, we construct QEC codes from the class of cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$.

Theorem 8: Let C be a cyclic code of length $6p^s$ over $\mathbb{F}_{p^m}$ which is of the form $\langle h_0(x)^{u_0} h_1(x)^{u_1} h_2(x)^{u_2} h_3(x)^{u_3} \rangle$, where $h_0(x) = x - 1, h_1(x) = x + 1, h_2(x) = x^2 - x + 1, h_3(x) = x^2 + x + 1$, and $0 \leq u_t \leq p^s$ $(t = 0, 1, 2, 3)$. If $0 \leq u_t < \frac{p^s}{2}$, then there exists a QEC code with parameters $[[6p^s, 6p^s - 2i_0 - 2i_1 - 4i_2 - 4i_3, \mathrm{d_H}(C)]]_{p^m}$. In this case, the number of QEC codes constructed from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using the CSS construction is $(\frac{p^s+1}{2})^4$.

Proof: Since $0 \leq u_0, u_1, u_2, u_3 < \frac{p^s}{2}$, by using Proposition 7, we have $C^{\perp} \subseteq C$. Using Theorem 6, there exists a QEC code with parameters $[[6p^s, 6p^s - 2i_0 - 2i_1 - 4i_2 - 4i_3, \mathrm{d_H}(C)]]_{p^m}$. Using Proposition 7, the number of dual-containing codes is $(\frac{p^s+1}{2})^4$. Hence, the number of QEC codes constructed from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using the CSS construction is $(\frac{p^s+1}{2})^4$. □

A construction which links between linear codes and QEC codes is the Steane's construction.

Theorem 9: (Steane's Construction [77]): Let C_1 and C_2 be two linear codes over $\mathbb{F}_{p^m}$ with parameters $[n, k_{C_1}, \mathrm{d_H}(C_1)]_{p^m}$ and $[n, k_{C_2}, \mathrm{d_H}(C_2)]_{p^m}$, where k_{C_1}, k_{C_2} are the dimensions of C_1 and C_2, respectively. If $C_1^{\perp} \subseteq C_1 \subseteq C_2$ and $k_{C_2} \geq k_{C_1} + 1$, then there exists an $[[n, k_{C_1} + k_{C_2} - n, \min\{\mathrm{d_H}(C_1), \lceil \frac{p^m+1}{p^m} \cdot \mathrm{d_H}(C_2) \rceil\}]]_{p^m}$ QEC code.

Combining Proposition 7 and Theorem 9, we construct QEC codes from the class of cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using the Steane's construction.

Theorem 10: Let C be a cyclic code of length $6p^s$ over $\mathbb{F}_{p^m}$ which is of the form $\langle h_0(x)^{u_0} h_1(x)^{u_1} h_2(x)^{u_2} h_3(x)^{u_3} \rangle$, where $h_0(x) = x - 1, h_1(x) = x + 1, h_2(x) = x^2 - x + 1, h_3(x) = x^2 + x + 1$ and $0 \leq u_t \leq p^s$ $(t = 0, 1, 2, 3)$. Let $C_1 = \langle h_0(x)^{u_0} h_1(x)^{u_1} h_2(x)^{u_2} h_3(x)^{u_3} \rangle$, $C_2 = \langle h_0(x)^{j_0} h_1(x)^{j_1} h_2(x)^{j_2} h_3(x)^{j_3} \rangle$ be cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$, where $0 \leq j_t, u_t \leq p^s$ $(t = 0, 1, 2, 3)$. If $k_{C_2} \geq k_{C_1} + 1$ and $0 \leq j_t \leq u_t < \frac{p^s}{2}$ $(t = 0, 1, 2, 3)$, then there exists a QEC code with parameters $[[6p^s, k_{C_1} + k_{C_2} - 6p^s, \min\{\mathrm{d_H}(C_1), \lceil \frac{p^m+1}{p^m} \cdot \mathrm{d_H}(C_2) \rceil\}]]_{p^m}$.

Proof: From $0 \leq j_t \leq u_t \leq p^s$ $(t = 0, 1, 2, 3)$, we have $C_1 \subseteq C_2$. By Proposition 7, we have $C_1^{\perp} \subseteq C_1$. Hence, $C_1^{\perp} \subseteq C_1 \subseteq C_2$. Using Theorem 9, there exists an $[[n, k_{C_1} + k_{C_2} - n, \min\{\mathrm{d_H}(C_1), \lceil \frac{p^m+1}{p^m} \cdot \mathrm{d_H}(C_2) \rceil\}]]_{p^m}$ QEC code. □

IV. QUANTUM MDS CODES

In 1992, The Singleton bound is given in [75] as follows: $|C| \leq p^{m(n-\mathrm{d_H}(C)+1)}$. The case of binary codes was first proved in [51]. Motivated by this, [48] also considered this problem. In 1974, the proof for general q-ary case is given by Denes and Keedwell [21]. A code C satisfying $|C| = p^{m(n-\mathrm{d_H}(C)+1)}$ which is called an MDS code. In 1952, Bush gave some results on MDS codes. After that, [36], [73] and [61] also provided several interesting results on MDS codes. The problem of the weight enumerator for such codes was considered by many researchers (for examples, [29], [60], [78]).

In 2020, [28] investigated the Hamming distances of cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ and provided all MDS constacyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ as follows.

Theorem 11: Let $C = \langle f^{\star}(x) \rangle$ be a cyclic code of length $6p^s$. Then C is an MDS code if and only if

- $\deg(f^{\star}(x)) = 0$, *in this case,* $\mathrm{d_H}(C) = 1$.
- $\deg(f^{\star}(x)) = 1$, *in this case,* $\mathrm{d_H}(C) = 2$.
- $\deg(f^{\star}(x)) = 6p^s - 1$, *in this case,* $\mathrm{d_H}(C) = 6p^s$.

Using Theorem 11, we give all MDS cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$.

Theorem 12: Let C be a cyclic code of length $6p^s$ over $\mathbb{F}_{p^m}$ which is of the form $\langle h_0(x)^{u_0}h_1(x)^{u_1}h_2(x)^{u_2}h_3(x)^{u_3}\rangle$, where $h_0(x) = x-1, h_1(x) = x+1, h_2(x) = x^2-x+1, h_3(x) = x^2+x+1$ and $0 \le u_t \le p^s$ $(t = 0, 1, 2, 3)$. Then C is an MDS cyclic code if and only if

- *$u_0 = u_1 = u_2 = u_3 = 0$, in this case, $\mathrm{d_H}(C) = 1$.*
- *$u_0 + u_1 + u_2 + u_3 = 1$, in this case, $\mathrm{d_H}(C) = 2$.*
- *$u_0 = p^s-1, u_1 = p^s, u_2 = p^s, u_3 = p^s$ or $u_0 = p^s, u_1 = p^s-1, u_2 = p^s, u_3 = p^s$, in this case, $\mathrm{d_H}(C) = 6p^s$.*

In the next part, we construct qMDS codes from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using the CSS construction. To do so, we recall the quantum Singleton bound for all classes of codes over finite fields as follows.

Theorem 16 (Quantum Singleton Bound) [38, Theorem 1]: Let $C = [[n, k, d_H]]_{p^m}$ be a QEC code. Then $k+2d_H \le n+2$.

If $k+2d_H = n+2$, then C is called a qMDS code. Since the Hamming distance of qMDS codes is maximal, these codes form an important class of QEC codes. Therefore, many researchers gave new qMDS codes (see [19], [38], [45]–[47], [49], [50], [56]).

Combining Theorems 7, 12 and 13, we construct qMDS codes from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ as follows.

Theorem 14: Let C be a cyclic code of length $6p^s$ over $\mathbb{F}_{p^m}$ which is of the form $\langle h_0(x)^{u_0}h_1(x)^{u_1}h_2(x)^{u_2}h_3(x)^{u_3}\rangle$, where $h_0(x) = x-1, h_1(x) = x+1, h_2(x) = x^2-x+1, h_3(x) = x^2+x+1$ and $0 \le u_t \le p^s$ $(t = 0, 1, 2, 3)$. Then the following statements hold:

- *If $u_0 = u_1 = u_2 = u_3 = 0$, then there exists a qMDS code with parameters $[[6p^s, 6p^s, 1]]_{p^m}$.*
- *If $u_0+u_1+u_2+u_3 = 1$, then there exists a qMDS code with parameters $[[6p^s, 6p^s-2, 2]]_{p^m}$.*

Proof: Let $C = \langle h_0(x)^{u_0}h_1(x)^{u_1}h_2(x)^{u_2}h_3(x)^{u_3}\rangle$ be an MDS cyclic code such that $C^\perp \subseteq C$. Then we see that $k_C = 6p^s - \mathrm{d_H}(C) + 1$ and $0 \le u_0, u_1, u_2, u_3 \le \frac{p^s}{2}$. From $C^\perp \subseteq C$, by applying Theorem 6 (the CSS construction), there exists a quantum code D with parameters $[[6p^s, 2k_C - 6p^s, \mathrm{d_H}(C)]]_{p^m}$. Since $k_C = 6p^s - \mathrm{d_H}(C) + 1$, we have $2k_C - 6p^s = 6p^s - 2\,\mathrm{d_H}(C) + 2$. By Theorem 13, D is a qMDS code with parameters $[[6p^s, 2k_C - 6p^s, \mathrm{d_H}(C)]]_{p^m}$. Hence, if $C = [6p^s, k_C, \mathrm{d_H}(C)]_{p^m}$ is an MDS cyclic code and $C^\perp \subseteq C$, then there exists a qMDS code with parameters $[[6p^s, 6p^s - 2\,\mathrm{d_H}(C)+2, \mathrm{d_H}(C)]]_{p^m}$. We consider 2 cases as follows:

Case 1: $u_0 = u_1 = u_2 = u_3 = 0$**.** In this case, we have $\mathrm{d_H}(C_{0,0}) = 1$. From Theorem 12, $C = [6p^s, 6p^s, 1]_{p^m}$ is an MDS cyclic code. From $u_0 = u_1 = u_2 = u_3 = 0$, we have $C^\perp \subseteq C$. As there exists a qMDS code with parameters $[[6p^s, 6p^s - 2\,\mathrm{d_H}(C)+2, \mathrm{d_H}(C)]]_{p^m}$, we have a qMDS code with parameters $[[6p^s, 6p^s, 1]]_{p^m}$.

Case 2: $u_0 + u_1 + u_2 + u_3 = 1$**.** In this case, we have $\mathrm{d_H}(C) = 2$. Applying Theorem 12, C is an MDS cyclic code. From $u_0 + u_1 + u_2 + u_3 = 1$, we have $C^\perp \subseteq C$. Hence, there exists a qMDS code with parameters $[[6p^s, 6p^s-2, 2]]_{p^m}$. □

V. QUANTUM SYNCHRONIZABLE CODES

QSCs are used for correcting the extract the Pauli errors on qubits and preventing the destruction of qubits in the quantum states. Therefore, several QSCs are provided to use in quantum synchronizable codes (for examples, [32], [34], [35], [79], [58], [59], [80]).

Let ℓ be an integer satisfying $\gcd(\ell, p) = 1$, where $\ell \ge 2$. Assume that $C_{t,\ell}$ is the cyclotomic coset of t modulo ℓ over $\mathbb{F}_q$ and denote by T_ℓ the set of representatives of all q-ary cyclotomic cosets. Let $f_t(x) = \prod_{i\in C_{t,\ell}}(x-\xi^i)$ be the minimal polynomial of ξ^t over $\mathbb{F}_q$, where ξ is a primitive ℓ-th root of unity in $\mathbb{F}_q$. Then the polynomial $x^{\ell p^s}-1$ over $\mathbb{F}_q$ can be factored as

$$x^{\ell p^s} - 1 = (x^\ell - 1)^{p^s} = \prod_{t\in T_\ell}(f_t(x))^{p^s}.$$

In 2015, by using the class of cyclic codes of length ℓp^s over $\mathbb{F}_q$, [58] constructed some QSCs.

Theorem 15 ([58, Theorem 3]): Let $C_1 = \langle\prod_{t\in T_\ell}(f_t(x))^{u_t}\rangle$ and $C_2 = \langle\prod_{t\in T_\ell}(f_t(x))^{j_t}\rangle$ be cyclic codes of length ℓp^s over $\mathbb{F}_{p^m}$ satisfying $C_1^\perp \subseteq C_1, C_2^\perp \subseteq C_2$, and $C_1 \subset C_2$. Then the following conditions hold:

(i) $u_t + i_{-t} \le p^s$.
(ii) $j_t + j_{-t} \le p^s$.
(iii) $0 \le j_t < u_t \le p^s$.

In such cases, if there exists an integer $r \in T_\ell$ with $\gcd(r, \ell) = 1$ satisfying either $i_r - j_r > p^{s-1}$ or $i_r - j_r > 0$ and $i_{r'} - j_{r'} > p^{s-1}$ for some $r' \ne r \in T_\ell$, then for any pair of non-negative integers a_b, a_e satisfying $a_b+a_e < \ell p^s$, there exists an (a_b, a_e)-$[[\ell p^s + a_b + a_e, \ell p^s - 2\sum_{t\in T_\ell} u_t|C_{t,\ell}|]]_q$ QSC.

Using Theorem 15, we construct QSCs from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ as follows.

Theorem 16: Let C be a cyclic code of length $6p^s$ over $\mathbb{F}_{p^m}$ which is of the form $\langle h_0(x)^{u_0}h_1(x)^{u_1}h_2(x)^{u_2}h_3(x)^{u_3}\rangle$, where $h_0(x) = x-1, h_1(x) = x+1, h_2(x) = x^2-x+1, h_3(x) = x^2+x+1$ and $0 \le u_t \le p^s$ $(t = 0, 1, 2, 3)$. Let $C_1 = \langle h_0(x)^{u_0}h_1(x)^{u_1}h_2(x)^{u_2}h_3(x)^{u_3}\rangle$, $C_2 = \langle h_0(x)^{j_0}h_1(x)^{j_1}h_2(x)^{j_2}h_3(x)^{j_3}\rangle$ be cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ satisfying $C_1^\perp \subseteq C_1$, $C_2^\perp \subseteq C_2$ and $C_1 \subset C_2$. Then the following conditions hold:

(i) $0 \le u_0, u_1, u_2, u_3 \le \frac{p^s}{2}$.
(ii) $0 \le j_0, j_1, j_2, j_3 \le \frac{p^s}{2}$.
(iii) $0 \le j_t < u_t \le p^s$, where $t = 0, 1, 2, 3$. In such cases, if there exists an integer $r \in T_6$ satisfying either $u_r - j_r > p^{s-1}$ or $u_r - j_r > 0$ and $u_{r'} - j_{r'} > p^{s-1}$ for some $r' \ne r \in T_6$, then for any pair of non-negative integers a_b, a_e satisfying $a_b + a_e < 6p^s$, there exists an $(a_b, a_e) - [[6p^s + a_b + a_e, 6p^s - 2u_0 - 2u_1 - 4u_2 - 4u_3]]_q$ QSC. If we fix u_t, j_t, r, where $t = 0, 1, 2, 3$ and $r \in T_6$, then there are $3p^s \cdot (6p^s+1)$ such QSCs.

TABLE 1. Known families of qMDS codes.

n	q	d	Reference
$n \leq q+1$	prime power	$d \leq \lfloor \frac{n}{2} \rfloor + 1$	[39]
$mq - l$	prime power	$d \leq m - l + 1, 0 \leq l < m, 1 < m < q$	[58]
$mq - l$	prime power	$3 \leq d \leq (q + 1 - \lfloor \frac{l}{m} \rfloor)/2, 0 \leq l \leq q-1, 1 \leq m \leq 4$	[48]
$r(q-1)+1$	$q \equiv r - 1\ (mod\ 2r)$	$d \leq \frac{q+r+1}{2}$	[49]
$q^2 - s$	prime power	$\frac{q}{2} + 1 < d \leq q - s$	[49]
$\frac{q^2+1}{2}$	q odd	$3 \leq d \leq q, d$ odd	[51]
$4 \leq n \leq q^2 + 1, n \neq 4$	$q \neq 2$	3	[48]
$q^2 - 1$	prime power	$d \leq q - l, 0 \leq l \leq q - 2$	[58]
$q^2 + 1$	prime power	$2 \leq d \leq q + 1$	[48], [51], [49]
$\frac{q^2-1}{2}$	q odd	$2 \leq d \leq q$	[52]
$\frac{q^2-1}{r}, r$ even, $r \neq 2, r \mid (q+1)$	q odd	$2 \leq d \leq \frac{q+1}{2}$	[52]
$\lambda(q+1), \lambda$ odd, $\lambda \mid (q-1)$	q odd	$2 \leq d \leq \frac{q+1}{2} + \lambda$	[52]
$2\lambda(q+1), \lambda$ odd, $\lambda \mid (q-1)$	$q \equiv 1\ (mod\ 4)$	$2 \leq d \leq \frac{q+1}{2} + 2\lambda$	[52]
$\frac{q^2+1}{5}$	$q \equiv 20m + 3, q \equiv 20m + 7$	$2 \leq d \leq \frac{q+5}{2}, d$ even	[52]
$\frac{q^2-1}{3}$	$3 \mid (q+1)$	$2 \leq d \leq \frac{2(q-2)}{3} + 1$	[19]
$\frac{q^2-1}{5}$	$5 \mid (q+1)$	$2 \leq d \leq \frac{3(q+1)}{5} - 1$	[19]
$\frac{q^2-1}{7}$	$7 \mid (q+1)$	$2 \leq d \leq \frac{4(q+1)}{7} - 1$	[19]
$\frac{q^2+1}{10}4$	$q = 10m + 3, q = 10m + 7$	$3 \leq d \leq 4m + 1, d$ odd	[19]
$n = 1 + \frac{r(q^2-1)}{2t+1}, 1 \leq t \in \mathbb{Z}, 1 \leq r \leq 2t+1$	$\gcd(r, q) = 1, q \equiv -1\ (mod\ 2t+1)$	$d \leq \frac{t+1}{2t+1} \times q - \frac{t}{2t+1} + 1$	[47]
$n = \frac{r(q^2-1)}{2t+1}, 1 \leq t \in \mathbb{Z}, 1 \leq r \leq 2t+1$	$\gcd(r, q) > 1, q \equiv -1\ (mod\ 2t+1)$	$d \leq \frac{t+1}{2t+1} \times q - \frac{t}{2t+1} + 1$	[47]
$2(d-1) \leq n \leq (d^2 - 2d + 2)$	prime power	$2 \leq d \leq q$	[47]

Proof: Since $C_1^{\perp} = \langle (x-1)^{p^s-u_0}(x+1)^{p^s-u_1}(x^2-x+1)^{u_2}(x^2+x+1)^{u_3} \rangle \subseteq C_1$ and $C_2^{\perp} = \langle (x-1)^{p^s-j_0}(x+1)^{p^s-j_1}(x^2-x+1)^{p^s-u_2}(x^2+x+1)^{p^s-u_3} \rangle \subseteq C_2$, we have $p^s - u_t \geq u_t, p^s - j_t \geq j_t$, where $t = 0, 1, 2, 3$, i.e., $0 \leq u_t \leq \frac{p^s}{2}$ and $0 \leq j_t \leq \frac{p^s}{2}$, showing (*i*) and (*ii*). From $C_1 \subseteq C_2$, it implies that $0 \leq j_t < u_t \leq p^s$, proving (*iii*). Since $C_1^{\perp} \subseteq C_1, C_2^{\perp} \subseteq C_2$, and $C_1 \subseteq C_2$, by using Theorem 15, if there is an integer $r \in T_6$ such that either $u_r - j_r > p^{s-1}$ or $u_r - j_r > 0$ and $u_{r'} - j_{r'} > p^{s-1}$ for some $r' \neq r \in T_6$, then for any pair of non-negative integers a_b, a_e satisfying $a_b + a_e < 6p^s$, there exists an $(a_b, a_e) - [[6p^s + a_b + a_e, 6p^s - 2u_0 - 2u_1 - 4u_2 - 4u_3]]_q$ QSC. Assume that u_t, j_t, r are fixed, where $t = 0, 1, 2, 3$ and $r \in T_6$. Using Lemma 5 for $n = 6p^s - 1$, there are $3p^s \cdot (6p^s + 1)$ pairs of non-negative integers a_b, a_e satisfying $a_b + a_e < 6p^s$. It means that there are $3p^s \cdot (6p^s + 1)$ such QSCs.

BCH codes are used in coding theory since they have useful in encoding and decoding algorithms. Let n be a divisor of $p^m - 1$ and γ be an element of $\mathbb{F}_{p^m}$ with multiplicative order n. A BCH code of length n is a cyclic code such that its generator polynomial has a set of $\alpha - 1$ consecutive roots $\gamma^e, \gamma^{e+1}, \cdots, \gamma^{e+\alpha-2}$, where $e \in \mathbb{N}^{\star}$. Applying the BCH bound, we see that the minimum distance of the BCH code is at least α. Therefore, the designed distance of the BCH code is α. If C is a BCH code satisfying the length $n = p^m - 1$, then C is called *primitive*. If $e = 1$, i.e., the $\alpha - 1$ consecutive roots start from γ, then C is called *narrow-sense*.

Remark 17: In 2015, [58, Table 2] gave some parameters of non-primitive, narrow-sense BCH codes C over $\mathbb{F}_q$ in Table 2. Some parameters of cyclic codes of length $6p^s$ over $\mathbb{F}_p$ are listed in Table 3 to show that the code lengths of cyclic codes of length $6p^s$ over $\mathbb{F}_p$ are smaller than BCH codes given in Table 2 but the Hamming distances of repeated-root cyclic codes of length $6p^s$ over $\mathbb{F}_p$ are better than γ_{max}, where γ_{max}

TABLE 2. Some parameters of non-primitive, narrow-sense BCH codes over $\mathbb{F}_p$.

p	length	δ_{max}
5	312	12
5	1562	60
7	8403	168
11	3660	30
13	92823	546

TABLE 3. Some parameters of cyclic codes of length $6p^s$ over $\mathbb{F}_p$.

p	s	C	length	d_H
5	2	$\langle h_0(x)^{24} h_1(x)^{25} h_2(x)^{25} h_3(x)^{25} \rangle$	150	150
5	3	$\langle h_0(x)^{125} h_1(x)^{124} h_2(x)^{125} h_3(x)^{125} \rangle$	750	750
7	3	$\langle h_0(x)^{342} h_1(x)^{343} h_2(x)^{343} h_3(x)^{343} \rangle$	2058	2058
11	2	$\langle h_0(x)^{121} h_1(x)^{120} h_2(x)^{121} h_3(x)^{121} \rangle$	726	726
13	3	$\langle h_0(x)^{2196} h_1(x)^{2197} h_2(x)^{2197} h_3(x)^{2197} \rangle$	13182	13182

is a precise lower bound for the largest minimum distance of a dual-containing BCH code. This is the reason why QSCs constructed from repeated-root cyclic codes of length $6p^s$ over $\mathbb{F}_p$ are better than QSCs constructed from non-primitive, narrow-sense BCH codes.

Put $h_0(x) = x - 1, h_1(x) = x + 1, h_2(x) = x^2 - x + 1, h_3(x) = x^2 + x + 1$. Then we have the following table.

VI. EXAMPLES

We start this section by providing some examples to illustrate Theorems 8 and 10.

Example 18: Let $p = 11$, $s = 1$ and $m = 1$. We have $x^{66} - 1 = h_0(x)^{11} h_1(x)^{11} h_2(x)^{11} h_3(x)^{11}$, where $h_0(x) = x - 1, h_1(x) = x + 1, h_2(x) = x^2 - x + 1, h_3(x) = x^2 + x + 1$.

(i) Let $C_1 = \langle h_0(x)^7 g_1(x)^2 g_3(x)^2 \rangle$ and $C_2 = \langle h_0(x)^6 g_1(x)^2 g_3(x)^2 \rangle$. Using Theorem 3.13 in [28], $d_H(C_1) = 4$ and $d_H(C_2) = 4$. It is easy to see that $k_{C_1} = 53$ and $k_{C_2} = 54$. By Theorem 10, we see that there exists a QEC code with parameters $[[66, 41, \min\{4, \lceil \frac{48}{11} \rceil\}]]_{11} = [[66, 41, 4]]_{11}$.

We compare the QEC code and online table [42] to see that the QEC code with parameters $[[66, 41, 4]]_{11}$ is new in the sense that the parameters are different from all the previous constructions.

(ii) Let $C_3 = \langle h_0(x)^2 g_1(x) h_3(x)\rangle$ and $C_4 = \langle g_0(x) h_1(x)\rangle$. It is easy to see that $C_3 \subseteq C_4$. We have $k_{C_3} = 61$ and $k_{C_4} = 64$. Using Theorem 3.13 in [28], $\mathrm{d_H}(C_3) = 3$ and $\mathrm{d_H}(C_4) = 2$. By Theorem 10, we see that there exists a QEC code with parameters $[[66, 59, \min\{3, \lceil \frac{24}{11} \rceil\}]]_{11} = [[66, 59, 3]]_{11}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[66, 59, 3]]_{11}$ is new in the sense that the parameters are different from all the previous constructions. Moreover, the QEC code with parameters $[[66, 59, 3]]_{11}$ is better than all QEC codes with same length and Hamming distance listed in [42], i.e., the QEC code constructed from cyclic code C_3 and C_4 using the Steane's construction has the dimension that is larger than the dimension of all QEC codes with same length and Hamming distance listed in [42].

(ii) Let $C_5 = \langle h_0(x)^3 g_1(x) h_3(x)\rangle$ and $C_6 = \langle g_0(x) g_1(x) h_3(x)\rangle$. It is easy to see that $C_5 \subseteq C_6$. We have $k_{C_5} = 60$ and $k_{C_6} = 61$. Using Theorem 3.13 in [28], $\mathrm{d_H}(C_5) = 4$ and $\mathrm{d_H}(C_6) = 3$. By Theorem 10, we see that there exists a QEC code with parameters $[[66, 55, \min\{4, \lceil \frac{36}{11} \rceil\}]]_{11} = [[66, 55, 4]]_{11}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[66, 55, 4]]_{11}$ is new in the sense that the parameters are different from all the previous constructions. Moreover, the QEC code with parameters $[[66, 55, 4]]_{11}$ is better than all QEC codes with same length and Hamming distance listed in [42], i.e., the QEC code constructed from cyclic code C_5 and C_6 using the Steane's construction has the dimension that is larger than the dimension of all QEC codes with same length and Hamming distance listed in [42].

Example 19: Let $p = 17, s = 1, m = 1$. We have $x^{102} - 1 = h_0(x)^{17} h_1(x)^{17} h_2(x)^{17} h_3(x)^{17}$, where $h_0(x) = x - 1, h_1(x) = x + 1, h_2(x) = x^2 - x + 1, h_3(x) = x^2 + x + 1$.

(*i*) Let $C_1 = \langle h_0(x)^3 g_1(x) h_3(x)\rangle$ and $C_2 = \langle h_0(x)^2 g_1(x) h_3(x)\rangle$. Hence, $C_1 \subseteq C_2$ and $k_{C_1} = 96, k_{C_2} = 97$. Applying Theorem 3.13 in [28], $\mathrm{d_H}(C_1) = 4$ and $\mathrm{d_H}(C_2) = 3$. From Proposition 7, it is easy to see that $C_1^{\perp} \subseteq C_1$. Using Theorem 8 for C_1, there exists a QEC code with parameters $[[102, 90, 4]]_{17}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[102, 90, 4]]_{17}$ is coincided with a QEC code listed in [42], i.e., it is not new in the sense that the parameters are different from all the previous constructions. However, by Theorem 10, we see that there exists a QEC code with parameters $[[102, 91, \min\{4, \lceil \frac{54}{17} \rceil\}]]_{17} = [[102, 91, 4]]_{17}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[102, 91, 4]]_{17}$ is new in the sense that the parameters are different from all the previous constructions. Moreover, the QEC code with parameters $[[102, 91, 4]]_{17}$ is better than all QEC codes with same length and Hamming distance listed in [42], i.e., the QEC code constructed from cyclic code C_1 and C_2 using the Steane's construction has the dimension that is larger than the dimension of all QEC codes with same length and Hamming distance listed in [42].

(*ii*) Let $C_3 = \langle h_0(x)^7 h_1(x)^3 g_2(x) h_3(x)^3\rangle$ and $C_4 = \langle h_0(x)^6 g_1(x)^3 g_3(x)\rangle$. Hence, $C_3 \subseteq C_4$ and $k_{C_3} = 84, k_{C_4} = 85$. Applying Theorem 3.13 in [28], $\mathrm{d_H}(C_3) = 8$ and $\mathrm{d_H}(C_4) = 7$. From Proposition 7, it is easy to see that $C_3^{\perp} \subseteq C_3$. Using Theorem 8 for C_3, there exists a QEC code with parameters $[[102, 66, 8]]_{17}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[102, 66, 8]]_{17}$ is coincided with a QEC code listed in [42], i.e., it is not new in the sense that the parameters are different from all the previous constructions. However, by Theorem 10, we see that there exists a QEC code with parameters $[[102, 67, \min\{8, \lceil \frac{126}{17} \rceil\}]]_{17} = [[102, 67, 8]]_{17}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[102, 67, 8]]_{17}$ is new in the sense that the parameters are different from all the previous constructions. Moreover, the QEC code with parameters $[[102, 67, 8]]_{17}$ is better than all QEC codes with same length and Hamming distance listed in [42], i.e., the QEC code constructed from cyclic code C_3 and C_4 using the Steane's construction has the dimension that is larger than the dimension of all QEC codes with same length and Hamming distance listed in [42].

(*iii*) Let $C_5 = \langle h_0(x)^8 h_1(x)^4 g_2(x)^2 g_3(x)^4\rangle$ and $C_6 = \langle h_0(x)^7 g_1(x)^3 g_2(x) h_3(x)^3\rangle$. Hence, $C_5 \subseteq C_6$ and $k_{C_5} = 78, k_{C_6} = 84$. Applying Theorem 3.13 in [28], $\mathrm{d_H}(C_5) = 9$ and $\mathrm{d_H}(C_6) = 8$. From Proposition 7, it is easy to see that $C_5^{\perp} \subseteq C_5$. Using Theorem 8 for C_5, there exists a QEC code with parameters $[[102, 54, 9]]_{17}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[102, 54, 9]]_{17}$ is coincided with a QEC code listed in [42], i.e., it is not new in the sense that the parameters are different from all the previous constructions. However, by Theorem 10, we see that there exists a QEC code with parameters $[[102, 60, \min\{9, \lceil \frac{144}{17} \rceil\}]]_{17} = [[102, 60, 9]]_{17}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[102, 60, 9]]_{17}$ is new in the sense that the parameters are different from all the previous constructions. Moreover, the QEC code with parameters $[[102, 60, 9]]_{17}$ is better than all QEC codes with same length and Hamming distance listed in [42], i.e., the QEC code constructed from cyclic code C_5 and C_6 using the Steane's construction has the dimension that is larger than the dimension of all QEC codes with same length and Hamming distance listed in [42].

Example 20: Let $p = 5$, $s = 2$ and $m = 1$. We have $x^{150} - 1 = h_0(x)^{25}h_1(x)^{25}h_2(x)^{25}h_3(x)^{25}$, where $h_0(x) = x - 1$, $h_1(x) = x + 1$, $h_2(x) = x^2 - x + 1$, $h_3(x) = x^2 + x + 1$.

(i) Let $C_1 = \langle h_0(x)^3 g_1(x)h_3(x)\rangle$. From Proposition 7, we see that $C_1^{\perp} \subseteq C_1$. Using Theorem 3.13 in [28], $\mathrm{d_H}(C_1) = 4$. By Theorem 8, there exists a QEC code with parameters $[[150, 138, 4]]_5$. We compare the QEC codes and online table [42] to see that the QEC codes with parameters $[[150, 138, 4]]_5$ is new in the sense that the parameters are different from all the previous constructions. Moreover, the QEC code with parameters $[[150, 138, 4]]_{17}$ is better than all QEC codes with same length and Hamming distance listed in [42], i.e., the QEC code constructed from cyclic code C_1 using CSS construction has the dimension that is larger than the dimension of all QEC codes with same length and Hamming distance listed in [42]. We see that the number of QEC codes constructed from all cyclic codes of length 150 over $\mathbb{F}_5$ using the CSS construction is 11325.

(ii) Let $C_2 = h_0(x)^2 f_1(x)h_3(x)$. Using Theorem 3.13 in [28], $\mathrm{d_H}(C_2) = 3$. It is easy to see that $k_{C_1} = 144$ and $k_{C_2} = 145$. By Theorem 10, we see that there exists a QEC code with parameters $[[150, 139, \min\{4, \lceil\frac{18}{5}\rceil\}]]_5 = [[150, 139, 4]]_5$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[150, 139, 4]]_5$ is new in the sense that the parameters are different from all the previous constructions. Moreover, the QEC code with parameters $[[150, 139, 4]]_5$ is better than all QEC codes with same length and Hamming distance listed in [42], i.e., the QEC code constructed from cyclic code C_1 and C_2 using the Steane's construction has the dimension that is larger than the dimension of all QEC codes with same length and Hamming distance listed in [42].

Example 21: Let $p = 23$, $s = 1$ and $m = 1$. We have $x^{138} - 1 = h_0(x)^{23}h_1(x)^{23}h_2(x)^{23}h_3(x)^{23}$, where $h_0(x) = x - 1$, $h_1(x) = x + 1$, $h_2(x) = x^2 - x + 1$, $h_3(x) = x^2 + x + 1$.

(i) Let $C_1 = \langle h_0(x)^6 g_1(x)^2 g_3(x)\rangle$ and $C_2 = \langle h_0(x)^5 g_1(x)^2 g_3(x)\rangle$. Using Theorem 3.13 in [28], $\mathrm{d_H}(C_1) = 4$ and $\mathrm{d_H}(C_2) = 4$. It is easy to see that $k_{C_1} = 127$ and $k_{C_2} = 129$. By Theorem 10, we see that there exists a QEC code with parameters $[[138, 118, \min\{4, \lceil\frac{96}{23}\rceil\}]]_{23} = [[138, 118, 4]]_{23}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[138, 118, 4]]_{23}$ is coincided with a QEC code listed in [42], i.e., it is not new in the sense that the parameters are different from all the previous constructions.

(ii) Let $C_3 = \langle h_0(x)^3 g_1(x)^2 g_3(x)\rangle$ and $C_4 = \langle h_0(x)^2 g_1(x)h_3(x)\rangle$. It is easy to see that $C_3 \subseteq C_4$. We have $k_{C_3} = 131$ and $k_{C_4} = 133$. Using Theorem 3.13 in [28], $\mathrm{d_H}(C_3) = 4$ and $\mathrm{d_H}(C_4) = 3$. By Theorem 10, we see that there exists a QEC code with parameters $[[138, 126, \min\{4, \lceil\frac{72}{23}\rceil\}]]_{23} = [[138, 124, 4]]_{23}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[138, 124, 4]]_{23}$ is new in the sense that the parameters are different from all the previous constructions. Moreover, the QEC code with parameters $[[150, 124, 4]]_{23}$ is better than all QEC codes with same length and Hamming distance listed in [42], i.e., the QEC code constructed from cyclic code C_3 and C_4 using the Steane's construction has the dimension that is larger than the dimension of all QEC codes with same length and Hamming distance listed in [42].

Example 22: Let $p = 29$, $s = 1$ and $m = 1$. We have $x^{174} - 1 = h_0(x)^{29}h_1(x)^{29}h_2(x)^{29}h_3(x)^{29}$, where $h_0(x) = x - 1$, $h_1(x) = x + 1$, $h_2(x) = x^2 - x + 1$, $h_3(x) = x^2 + x + 1$.

(i) Let $C_1 = \langle h_0(x)^7 f_1(x)^2 f_3(x)^2\rangle$ and $C_2 = \langle h_0(x)^6 f_1(x)^2 f_3(x)^2\rangle$. Using Theorem 3.13 in [28], $\mathrm{d_H}(C_1) = 4$ and $\mathrm{d_H}(C_2) = 4$. It is easy to see that $k_{C_1} = 161$ and $k_{C_2} = 162$. By Theorem 10, we see that there exists a QEC code with parameters $[[174, 149, \min\{4, \lceil\frac{120}{29}\rceil\}]]_{29} = [[174, 149, 4]]_{29}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[174, 149, 4]]_{29}$ is coincided with a QEC code listed in [42], i.e., it is not new in the sense that the parameters are different from all the previous constructions.

(ii) Let $C_3 = \langle h_0(x)^3 f_1(x)^2 f_3(x)\rangle$ and $C_4 = \langle h_0(x)^2 f_1(x)h_3(x)\rangle$. It is easy to see that $C_3 \subseteq C_4$. We have $k_{C_3} = 167$ and $k_{C_4} = 169$. Using Theorem 3.13 in [28], $\mathrm{d_H}(C_3) = 4$ and $\mathrm{d_H}(C_4) = 3$. By Theorem 10, we see that there exists a QEC code with parameters $[[174, 162, \min\{4, \lceil\frac{90}{29}\rceil\}]]_{29} = [[174, 162, 4]]_{29}$. We compare the QEC code and online table [42] to see that the QEC code with parameters $[[174, 162, 4]]_{29}$ is new in the sense that the parameters are different from all the previous constructions. Moreover, the QEC code with parameters $[[174, 162, 4]]_{29}$ is better than all QEC codes with same length and Hamming distance listed in [42], i.e., the QEC code constructed from cyclic code C_3 and C_4 using the Steane's construction has the dimension that is larger than the dimension of all QEC codes with same length and Hamming distance listed in [42].

Example 23: Let $p = 11$, $s = 1$, $m = 1$. We see that $x^{66} - 1 = h_0(x)^{11}h_1(x)^{11}h_2(x)^{11}h_3(x)^{11}$, where $h_0(x) = x - 1$, $h_1(x) = x + 1$, $h_2(x) = x^2 - x + 1$, $h_3(x) = x^2 + x + 1$.

(*i*) Let $C_0 = \langle 1\rangle$. By Proposition 7, it is easy to see that $C_0^{\perp} \subseteq C_0$. By using Theorem 14, we see that there is a qMDS code with parameters $[[66, 66, 1]]_{11}$.

(*ii*) Let $C_1 = \langle (x - 1)\rangle$. From Proposition 7, it is easy to see that $C_1^{\perp} \subseteq C_1$. From Theorem 14, we see that there is a qMDS code with parameters $[[66, 64, 2]]_{11}$.

(*ii*) Let $C_2 = \langle (x + 1)\rangle$. From Proposition 7, it is easy to see that $C_1^{\perp} \subseteq C_1$. By using Theorem 14, we see that there is a qMDS code with parameters $[[66, 64, 2]]_{11}$.

Example 24: Let $p = 11$, $s = 2$, $m = 1$. We see that $x^{726} - 1 = h_0(x)^{121}h_1(x)^{121}h_2(x)^{121}h_3(x)^{121}$, where $h_0(x) = x - 1$, $h_1(x) = x + 1$, $h_2(x) = x^2 - x + 1$, $h_3(x) = x^2 + x + 1$.

(*i*) Let $C_0 = \langle 1\rangle$. By Proposition 7, it is easy to see that $C_0^{\perp} \subseteq C_0$. By using Theorem 14, we see that there is a qMDS code with parameters $[[726, 726, 1]]_{11}$.

(*ii*) Let $C_1 = \langle (x-1)\rangle$. From Proposition 7, it is easy to see that $C_1^{\perp} \subseteq C_1$. From Theorem 14, we see that there is a qMDS code with parameters $[[726, 724, 2]]_{11}$.

(*ii*) Let $C_2 = \langle (x+1)\rangle$. From Proposition 7, it is easy to see that $C_1^{\perp} \subseteq C_1$. By using Theorem 14, we see that there is a qMDS code with parameters $[[726, 724, 2]]_{11}$.

Example 25: Let $p = 29, s = 1, m = 1$. We have $x^{174} - 1 = h_0(x)^{29}h_1(x)^{29}h_2(x)^{29}h_3(x)^{29}$, where $h_0(x) = x-1, h_1(x) = x+1, h_2(x) = x^2-x+1, h_3(x) = x^2+x+1$.

(*i*) Let $C_0 = \langle 1\rangle$. From Theorem 3.2, it is easy to see that $C_0^{\perp} \subseteq C_0$. Using Theorem 14, we see that there is a qMDS code with parameters $[[124, 124, 1]]_{29}$.

(*ii*) Let $C_1 = \langle (x+1)\rangle$. From Proposition 7, it is easy to see that $C_1^{\perp} \subseteq C_1$. Applying Theorem 14, we see that there is a qMDS code with parameters $[[124, 122, 2]]_{29}$.

Example 26: Let $p = 29$, $s = 2, m = 1$. We have $x^{5046} - 1 = h_0(x)^{841}h_1(x)^{841}h_2(x)^{841}h_3(x)^{841}$, where $h_0(x) = x - 1, h_1(x) = x+1, h_2(x) = x^2-x+1, h_3(x) = x^2+x+1$.

(*i*) Let $C_0 = \langle 1\rangle$. From Proposition 3.3, it is easy to see that $C_0^{\perp} \subseteq C_0$. By applying Theorem 14, there is a qMDS code with parameters $[[5046, 5046, 1]]_{29}$.

(*ii*) Let $C_1 = \langle (x+1)\rangle$. From Proposition 7, it is easy to see that $C_1^{\perp} \subseteq C_1$. By using Theorem 14, there is a qMDS code with parameters $[[5046, 5044, 2]]_{29}$.

Remark 27: We can compare our qMDS codes and known families of qMDS codes (Table 1) and [42] to see that our qMDS codes are new in the sense that their parameters are different from all the known ones.

We finish this section by giving some examples of QSCs.

Example 28: Let $p = 17, s = 1, m = 1$. We see that $x^{102} - 1 = h_0(x)^{17}h_1(x)^{17}h_2(x)^{17}h_3(x)^{17}$, where $h_0(x) = x-1, h_1(x) = x+1, h_2(x) = x^2-x+1, h_3(x) = x^2+x+1$.

- If $C_1 = \langle f_0(x)h_1(x)^8h_2(x)^5h_3(x)^3\rangle$ and $C_2 = \langle h_1(x)^2f_2(x)h_3(x)\rangle$, then $C_1^{\perp} \subseteq C_1$, $C_2^{\perp} \subseteq C_2$ and $C_1 \subseteq C_2$. We see that $u_3 - j_3 > 1$. Applying Theorem 16, for any pair a_b, a_e of non-negative integers satisfying $a_b + a_e < 102$, there exists an $(a_b, a_e) - [[102 + a_b + a_e, 52]]_{17}$ QSC. In this case, there are 5253 such QSCs.
- If $C_3 = \langle h_0(x)^5f_1(x)^7f_2(x)^5f_3(x)^3\rangle$ and $C_4 = \langle f_0(x)f(x)f_2(x)h_3(x)^2\rangle$, then $C_3^{\perp} \subseteq C_3$, $C_4^{\perp} \subseteq C_4$ and $C_3 \subseteq C_4$. We see that $u_1 - j_1 > 1$. Applying Theorem 16, for any pair a_b, a_e of non-negative integers satisfying $a_b + a_e < 102$, there exists an $(a_b, a_e) - [[102 + a_b + a_e, 46]]_{17}$ QSC. In this case, there are 5253 such QSCs.

Example 29: Let $p = 17, s = 2, m = 1$. We see that $x^{1734} - 1 = h_0(x)^{289}h_1(x)^{289}h_2(x)^{289}h_3(x)^{289}$, where $h_0(x) = x-1, h_1(x) = x+1, h_2(x) = x^2-x+1, h_3(x) = x^2+x+1$. If $C_1 = \langle h_0(x)^{19}h_1(x)^{109}h_2(x)^{38}h_3(x)^{24}\rangle$ and $C_2 = \langle h_0(x)^8h_1(x)^{12}h_2(x)^6h_3(x)^4\rangle$, then $C_1^{\perp} \subseteq C_1$, $C_2^{\perp} \subseteq C_2$ and $C_1 \subseteq C_2$. We see that $u_3 - j_3 > 17$. Applying Theorem 16, for any pair a_b, a_e of non-negative integers satisfying $a_b + a_e < 1734$, there exists an $(a_b, a_e) - [[1734 + a_b + a_e, 1230]]_{17}$ QSC. By applying Lemma 5, there are 1504245 such QSCs.

Example 30: Let $p = 23, s = 1, m = 1$. We see that $x^{138} - 1 = h_0(x)^{23}h_1(x)^{23}h_2(x)^{23}h_3(x)^{23}$, where $h_0(x) = x-1, h_1(x) = x+1, h_2(x) = x^2-x+1, h_3(x) = x^2+x+1$.

- If $C_1 = \langle f_0(x)h_1(x)^8h_2(x)^6h_3(x)^5\rangle$ and $C_2 = \langle h_1(x)^2h_2(x)^3\rangle$, then $C_1^{\perp} \subseteq C_1$, $C_2^{\perp} \subseteq C_2$ and $C_1 \subseteq C_2$. We see that $u_3 - j_3 > 1$. Applying Theorem 16, for any pair a_b, a_e of non-negative integers satisfying $a_b + a_e < 138$, there exists an $(a_b, a_e) - [[138 + a_b + a_e, 88]]_{23}$ QSC. Using Lemma 5, there are 9591 such QSCs.
- If $C_3 = \langle h_0(x)^5h_1(x)^6h_2(x)^4h_3(x)^3\rangle$ and $C_4 = \langle f_0(x)f_1(x)f_2(x)h_3(x)^2\rangle$, then $C_3^{\perp} \subseteq C_3$, $C_4^{\perp} \subseteq C_4$ and $C_3 \subseteq C_4$. We see that $u_1 - j_1 > 1$. Applying Theorem 16, for any pair a_b, a_e of non-negative integers satisfying $a_b + a_e < 138$, there exists an $(a_b, a_e) - [[138 + a_b + a_e, 88]]_{23}$ QSC. By using Lemma 5, we see that there are 9591 such QSCs.

Example 31: Let $p = 23, s = 2, m = 1$. We have $x^{3174} - 1 = h_0(x)^{529}h_1(x)^{529}h_2(x)^{529}h_3(x)^{529}$, where $h_0(x) = x - 1, h_1(x) = x+1, h_2(x) = x^2-x+1, h_3(x) = x^2+x+1$.

- If $C_1 = \langle f_0(x)h_1(x)^{48}h_2(x)^{26}h_3(x)^{15}\rangle$ and $C_2 = \langle h_1(x)^{12}h_2(x)^9\rangle$, then $C_1^{\perp} \subseteq C_1$, $C_2^{\perp} \subseteq C_2$ and $C_1 \subseteq C_2$. We see that $u_3 - j_3 > 1$. Applying Theorem 16, for any pair a_b, a_e of non-negative integers satisfying $a_b + a_e < 3174$, there exists an $(a_b, a_e) - [[3174 + a_b + a_e, 2912]]_{23}$ QSC. Applying Lemma 5, there are 5040312 such QSCs.
- If $C_3 = \langle h_0(x)^{45}h_1(x)^{16}h_2(x)^{24}h_3(x)^{33}\rangle$ and $C_4 = \langle f_0^6(x)f_1(x)^9f_2(x)^7g_3(x)^2\rangle$, then $C_3^{\perp} \subseteq C_3$, $C_4^{\perp} \subseteq C_4$ and $C_3 \subseteq C_4$. We see that $u_1 - j_1 > 1$. Applying Theorem 16, for any pair a_b, a_e of non-negative integers satisfying $a_b + a_e < 3174$, there exists an $(a_b, a_e) - [[3174 + a_b + a_e, 2938]]_{23}$ QSC. Using Lemma 5, there are 5040312 such QSCs.

VII. CONCLUSION

In this paper, we use the CSS and Steane's constructions to establish QEC codes from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ (Theorems 8 and 10). We get some new QEC codes in the sense that the parameters are different from all the previous constructions (Examples 3.6 and 3.7). Applying the quantum Singleton bound, all qMDS cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using the CSS construction are determined in Theorem 14. As in Section 5, we construct QSCs from cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ (Theorem 16) and such codes are applicable in quantum synchoronizable. Remark 17 shows that QSCs constructed from repeated-root cyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ are better than QSCs constructed from non-primitive, narrow-sense BCH codes. In Section 6, we provide some examples to illustrate our work in Sections 3, 4 and 5.

Although we only consider the case $p^m \equiv 2 \pmod 3$ in this paper, the situation of $p^m \equiv 1 \pmod 3$ can be studied in a similar fashion. When $p^m \equiv 1 \pmod 3$, from [26], all cyclic codes of length $6p^s$ have the form $C = \langle (x-1)^{u_0}(x+1)^{u_1}(x-\xi^{\frac{p^m-1}{6}})^{u_2}(x-\xi^{\frac{5(p^m-1)}{6}})^{u_3}(x-\xi^{\frac{2(p^m-1)}{6}})^{u_4}(x-\xi^{\frac{4(p^m-1)}{6}})^{u_5}\rangle$, where $0 \leq u_t \leq p^s$ ($t = 0, 1, 2, 3, 4, 5$) and $\xi \in \mathbb{F}_{p^m}$ is a primitive (p^m-1)th root of unity. Applying the method used in [28], we can determine the Hamming distances of all such cyclic codes. We also compute all Hamming distances of negacyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$. Similar to Theorems 8 and 10, we can construct new QEC codes from cyclic and negacyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$ using the CSS and Steane's constructions.

Let $q = p^m$ and $\mathbb{F}_{q^2}$ be a finite field of q^2 elements. If $e = (e_0, e_1, \ldots, e_{n-1}), t = (t_0, t_1, \cdots, t_{n-1})$ are two vectors of $\mathbb{F}_{q^2}$, then Hermitian inner product of e and t is

$$e \circ_{\mathbb{F}_{q^2}} t = e_0\bar{t}_0 + e_1\bar{t}_1 + \cdots + e_{n-1}\bar{t}_{n-1},$$

where $\bar{t}_i = t_i^q$. The Hermitian dual code of C is defined as

$$C^{\perp_H} = \{e \in \mathbb{F}_{q^2}^n | \sum_{i=0}^{n-1} e_i\bar{t}_i = 0, \forall t \in C\}.$$

If $C^{\perp_H} \subseteq C$, then C is said to be *Hermitian dual-containing*.

The Hermitian construction is also an important construction appeared in [1].

Theorem 32 (Hermitian Construction [1]): Let $C = [n, k, d_H]$ be a q^2-ary linear code satisfying $C^{\perp_H} \subseteq C$. Then there exists a q-ary quantum code with parameters $[[n, 2k-n, \geq d_H]]_q$.

By giving the condition of a cyclic and negacyclic code of length $6p^s$ over $\mathbb{F}_{q^2}$ to construct QEC codes, similar to Theorem 14, we can construct new QEC codes from cyclic and negacyclic codes of length $6p^s$ over $\mathbb{F}_{q^2}$ using the Hermitian construction.

We also investigate the QSCs constructed from negacyclic codes of length $6p^s$ over $\mathbb{F}_{p^m}$, or more generally $2^m p^s$, for any non-negative integer m in near future. We believe that these lengths can provide good and new QEC codes and QSCs.

ACKNOWLEDGMENT

The authors sincerely thank the reviewers and the editor for their helpful comments and valuable suggestions, which have greatly improved the presentation of this paper.

REFERENCES

[1] A. Ashikhmin and E. Knill, "Nonbinary quantum stablizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, Nov. 2001.

[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wooters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A, Gen. Phys.*, vol. 54, p. 3824, Nov. 1996.

[3] S. D. Berman, "Semisimple cyclic and Abelian codes. II," *Kibernetika*, vol. 3, no. 3, pp. 21–30, 1967.

[4] S. Bregni, *Synchronization of Digital Telecommunications Networks*. New York, NY, USA: Wiley, 2002.

[5] K. A. Bush, "Orthogonal arrays of index unity," *Ann. Math. Statist.*, vol. 23, no. 3, pp. 426–434, 1952.

[6] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1106, Aug. 1996.

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.

[8] Y. Cao, Y. Cao, H. Q. Dinh, F. Fu, J. Gao, and S. Sriboonchitta, "Constacyclic codes of length np^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$," *Adv. Math. Commun.*, vol. 12, no. 2, pp. 231–262, 2018.

[9] Y. Cao, Y. Cao, H. Q. Dinh, F. Fu, J. Gao, and S. Sriboonchitta, "A class of repeated-root constacyclic codes over $\mathbb{F}_{p^m}[u]/\langle u^e\rangle$ of type 2," *Finite Fields Appl.*, vol. 55, pp. 238–267, Jan. 2019.

[10] Y. Cao, Y. Cao, H. Q. Dinh, and S. Jitman, "An explicit representation and enumeration for self-dual cyclic codes over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ of length 2^s," *Discrete Math.*, vol. 342, pp. 2077–2091, Jul. 2019.

[11] Y. Cao, Y. Cao, H. Q. Dinh, F. Fu, J. Gao, and S. Sriboonchitta, "A class of linear codes of length 2 over finite chain rings," *J. Algebra Appl.*, vol. 19, Jun. 2020, Art. no. 2050103.

[12] Y. Cao, Y. Cao, H. Q. Dinh, F. Fu, and F. Ma, "Construction and enumeration for self-dual cyclic codes of even length over $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$," *Finite Fields Appl.*, vol. 15, no. 2, pp. 291–309, May 2021.

[13] Y. Cao, Y. Cao, H. Q. Dinh, F. Fu, and F. Ma, "On matrix-product structure of repeated-root constacyclic codes over finite fields," *Discrete Math*, vol. 343, Apr. 2020, Art. no. 111768.

[14] Y. Cao, Y. Cao, H. Q. Dinh, R. Bandi, and F. Fu, "An explicit representation and enumeration for negacyclic codes of length $2^k n$ over $\mathbb{Z}_4+u\mathbb{Z}_4$," *Adv. Math. Commun.*, vol. 15, no. 2, p. 291, 2020.

[15] Y. Cao, Y. Cao, H. Q. Dinh, T. Bag, and W. Yamaka, "Explicit representation and enumeration of repeated-root $\delta^2+\alpha u^2$-constacyclic codes over $\mathbb{F}_{2^m}[u]/\langle u^{2\lambda}\rangle$," *IEEE Access*, vol. 8, pp. 55550–55562, 2020.

[16] Y. Cao, Y. Cao, H. Q. Dinh, and S. Jitman, "An efcient method to construct self-dual cyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$," *Discrete Math.*, vol. 343, Jun. 2020, Art. no. 111868.

[17] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, "On repeated-root cyclic codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 337–342, Mar. 1991.

[18] B. Chen, H. Q. Dinh, and H. Liu, "Repeated-root constacyclic codes of length ℓp^s and their duals," *Discrete Appl. Math.*, vol. 177, pp. 60–70, Nov. 2014.

[19] B. Chen, S. Ling, and G. Zhang, "Application of constacyclic codes to quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1474–1478, Mar. 2014.

[20] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 1, p.76, 1997.

[21] J. Denes and A. D. Keedwell, *Latin Squares and Their Applications*. New York, NY, USA: Academic, 1974.

[22] D. Deutsch, "Quantum theory, the church–turning principle and the universal quantum computer," *Proc. Roy. Soc. London. A. Math. Phys. Sci.*, vol. 400, no. 1818, pp. 97–117, Jul. 1985.

[23] H. Q. Dinh, "Constacyclic codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$," *J. Algebra*, vol. 324, pp. 940–950, Sep. 2010.

[24] H. Q. Dinh, "Repeated-root constacyclic codes of length $2p^s$," *Finite Fields Appl.*, vol. 18, pp. 133–143, Jan. 2012.

[25] H. Q. Dinh, "Structure of repeated-root constacyclic codes of length $3p^s$ and their duals," *Discrete Math.*, vol. 313, pp. 983–991, May 2013.

[26] H. Q. Dinh, "Repeated-root cyclic and negacyclic codes of length $6p^s$," *Contemp. Math.*, vol. 609, pp. 69–87, Feb. 2014.

[27] H. Q. Dinh, B. T. Nguyen, and W. Yamaka, "Quantum MDS and synchronizable codes from cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$," *IEEE Access*, vol. 8, pp. 124608–124623, 2020.

[28] H. Q. Dinh, X. Wang, and P. Maneejuk, "On the Hamming distance of repeated-root cyclic codes of length $6p^s$," *IEEE Access*, vol. 8, pp. 39946–39958, 2020.

[29] M. El-Khamy and R. J. McEliece, "The partition weight enumerator of MDS codes and its applications," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Sep. 2005, pp. 926–930.

[30] W. Fang and F.-W. Fu, "Two new classes of quantum MDS codes," *Finite Fields Appl.*, vol. 53, pp. 85–98, Sep. 2018.

[31] W. Fang and F. Fu, "Some new constructions of quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 7840–7847, Sep. 2019.

[32] Y. Fujiwara, "Block synchronization for quantum information," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 2, pp. 109–120, Feb. 2013.
[33] Y. Fujiwara and D. Tonchev, "High-rate self-synchronizing codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2328–2335, Dec. 2013.
[34] Y. Fujiwara, V. D. Tonchev, and T. W. H. Wong, "Algebraic techniques in designing quantum synchronizable codes," *Phys. Rev. A, Gen. Phys.*, vol. 88, no. 1, pp. 162–166, Jul. 2013.
[35] Y. Fujiwara and P. Vandendriessche, "Quantum synchronizable codes from finite geometries," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7345–7354, Nov. 2014.
[36] S. Golomb and E. Posner, "Rook domains, Latin squares, affine planes, and error-distributing codes," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 3, pp. 196–208, Jul. 1964.
[37] D. Gottesman, M.S. thesis, California Inst. Technol. (Caltech), Pasadena, CA, USA, quantph/9705052, 1997.
[38] M. Grassl, T. Beth, and M. R. otteler, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 2, pp. 757–766, Mar. 2004.
[39] M. Grassl, A. Klappenecker, and M. Rotteler, "Graphs, quadratic forms, and quantum codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2002, p. 45.
[40] M. Grassl, T. Beth, and W. Geiselmann, "Quantum Reed–Solomon codes," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Honolulu, HI, USA: AAECC-13, 1999.
[41] M. Grassl and T. Beth, "Quantum BCH codes," in *Proc. 10th Int. Symp.*, Magdeburg, Germany, 1999, pp. 207–212.
[42] M. Grassl. *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. Accessed: Apr. 3, 2021. [Online]. Available: https://www.codetables.de
[43] G. G. La Guardia, "Constructions of new families of nonbinary quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 80, no. 4, Oct. 2009, Art. no. 042331.
[44] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu, and C. H. Oh, "Graphical nonbinary quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 1, pp. 1–11, Jul. 2008.
[45] L. Jin, H. Kan, and J. Wen, "Quantum MDS codes with relatively large minimum distance from Hermitian self-orthogonal codes," *Des., Codes Cryptogr.*, vol. 84, no. 3, pp. 463–471, 2017.
[46] L. Jin, S. Ling, J. Luo, and C. Xing, "Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4735–4740, Sep. 2010.
[47] L. Jin and C. Xing, "A construction of new quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2921–2925, May 2014.
[48] D. D. Joshi, "A note on upper bounds for minimum distance codes," *Inf. Control*, vol. 1, no. 3, pp. 289–295, Sep. 1958.
[49] X. Kai and S. Zhu, "New quantum MDS codes from negacyclic codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1193–1197, Feb. 2013.
[50] X. Kai, S. Zhu, and P. Li, "A construction of new MDS symbol-pair codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 5828–5834, Nov. 2015.
[51] Y. Komamiya, "Application of logical mathematics to information theory," in *Proceedings of the Third Japan National Congress for Applied Mechanics* (Application of Theory of Groups to Logical Mathematics). Tokyo, Japan: Science Council of Japan, 1954. pp. 437–442.
[52] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 2, pp. 900–911, Feb. 1997.
[53] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. Lett.*, vol. 84, p. 2525, Feb. 2000.
[54] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, no. 1, p. 198, 1996.
[55] A. Lidar and A. Brun. *Quantum Error Correction*. Cambridge, U.K.: Cambridge Univ. Press, 2013.
[56] Z. Li, L.-J. Xing, and X.-M. Wang, "Quantum generalized Reed–Solomon codes: Unified framework for quantum maximum-distance-separable codes," *Phys. Rev. A, Gen. Phys.*, vol. 77, no. 1, pp. 1–4, Jan. 2008.
[57] J. H. van Lint, "Repeated-root cyclic codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 343–345, Mar. 1991.
[58] L. Luo and Z. Ma, "Non-binary quantum synchronizable codes from repeated-root cyclic codes," *IEEE Trans. Inf. Theory*, vol. 14, no. 3, pp. 1–10, Jan. 2015.
[59] L. Luo, Z. Ma, and D. Lin, "Two new families of quantum synchronizable codes," *Quantum Inf. Process.*, vol. 18, no. 9, pp. 1–18, Sep. 2019.
[60] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 10th ed. Amsterdam, The Netherlands: Impression, 1998.
[61] C. Maneri and R. Silverman, "A combinatorial problem with applications to geometry," *J. Combinat. Theory A*, vol. 11, no. 2, pp. 118–121, Sep. 1971.
[62] J. L. Massey, D. J. Costello, and J. Justesen, "Polynomial weights and code constructions," *IEEE Trans. Inf. Theory*, vol. IT-19, no. 1, pp. 101–110, Jan. 1973.
[63] A. Nielsen and L. Chuang, *Quantum Computation and Quantum Information*, Cambridge, U.K.: Cambridge Univ. Press, 2010.
[64] V. Pless and W. C. Huffman, *Handbook of Coding Theory*. Amsterdam, The Netherlands: Elsevier, 1998.
[65] Y. Polyanskiy, "Asynchronous communication: Exact synchronization, universality, and dispersion," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1256–1270, Mar. 2013.
[66] E. Prange, "Cyclic error-correcting codes in two symbols," Tech. Rep. TN-57-103, Sep. 1957.
[67] E. M. Rains, "Quantum weight enumerators," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1388–1394, Jul. 1998.
[68] R. M. Roth and G. Seroussi, "On cyclic MDS codes of length q over GF(q)," *IEEE Trans. Inf. Theory*, vol. IT-32, no. 2, pp. 284–285, Mar. 1986.
[69] D. Schlingemann and R. F. Werner, "Quantum error-correcting codes associated with graphs," *Phys. Rev. A, Gen. Phys.*, vol. 65, Dec. 2001, Art. no. 012308.
[70] D. Schlingemann, "Stabilizer codes can be realized as graph codes," *Quantum Inf. Comput.*, vol. 2, no. 4, pp. 307–323, Jun. 2002.
[71] X. Shi, Q. Yue, and X. Zhu, "Construction of some new quantum MDS codes," *Finite Fields Their Appl.*, vol. 46, pp. 347–362, Jul. 2017.
[72] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, p. 2493, Oct. 1995.
[73] R. Silverman, "A metrization for power-sets with applications to combinatorial analysis," *Can. J. Math.*, vol. 12, pp. 158–176, 1960.
[74] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.
[75] R. Steven, *Coding and Information Theory*. Springer-Verlag, 1992.
[76] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, p. 793, 1996.
[77] A. M. Steane, "Enlargement of Calderbank–Shor–Steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999.
[78] L. M. G. M. Tolhuizen, "On maximum distance separable codes over alphabets of arbitrary size," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 1994, p. 431.
[79] Y. Xie, J. Yuan, and Y. Fujiwara, "Quantum synchronizable codes from augmentation of cyclic codes," *PLoS ONE*, vol. 6, p. e14641, Apr. 2014.
[80] Y. Xie, L. Yang, and J. Yuan, "Q-ary chain-containing quantum synchronizable codes," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 414–417, Mar. 2016.
[81] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.
[82] T. Zhang and G. Ge, "Some new classes of quantum MDS codes from constacyclic codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 5224–5228, Sep. 2015.
[83] T. Zhang and G. Ge, "Quantum MDS codes with large minimum distance," *Des., Codes Cryptogr.*, vol. 83, no. 3, pp. 503–517, Jun. 2017.